



Для служебного пользования
Экз. №1

**Общество с ограниченной ответственностью
«ПНК»**

(Лицензия ФСТЭК России № 1393 от 9 марта 2011 г.)

УТВЕРЖДАЮ
Генеральный директор
ООО «ПНК»
ПНК
А. Л. Коваль
«05» июля 2023 г.

МБДОУ «ДС № 332 г. Челябинска»

**Объект информатизации
информационная система персональных данных
«ГРАЖДАНЕ»**

Заключение по результатам оценки соответствия

г. Челябинск
2023 г.

Уч. № 4379-04дсп

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Комиссия, в которую включены эксперты по соответствующим направлениям, сформированная ООО «ПНК», (Лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации № 1393 от 9 марта 2011 г.) в составе:

Рублев Е.Л. – директор по информационной безопасности ООО «ПНК», председатель комиссии;

Мисбахова К.А. – начальник отдела защиты информационных систем ООО «ПНК», член комиссии;

Щетин А.И. – заместитель начальника отдела электронных торгов ООО «ПНК», член комиссии

провела испытания, результаты которых приведены в протоколе оценки соответствия требованиям безопасности информации по направлению «Защита информации от несанкционированного доступа» (уч. № 4379-03дсп от 05.07.2023).

1.2. Заявитель испытаний объекта – МБДОУ «ДС № 332 г. Челябинска» (далее – Заявитель).

2. ЦЕЛЬ, ОБЪЕКТЫ И УСЛОВИЯ ИСПЫТАНИЙ

2.1. Целью испытаний является определение соответствия объекта информатизации Заявителя требованиям безопасности информации. Испытания проводятся на соответствие положениям и требованиям действующих нормативных правовых актов, методических документов и национальных стандартов в области защиты информации.

2.2. Объект испытаний – информационная система персональных данных (далее – ИСПДн) на базе одного ПЭВМ «Граждане», установленная в МБДОУ «ДС № 332 г. Челябинска», расположенная по адресу: Челябинская область, город Челябинск, улица Барбюса, дом 144Г, методический кабинет (далее объект информатизации – ОИ).

2.3. При проведении испытаний применялись следующие методы проверок и испытаний:

– экспертно-документальный метод, предусматривающий проверку соответствия ИСПДн требованиям по безопасности информации на основании экспертной оценки полноты и достаточности представленных документов по обеспечению необходимых мер защиты информации в ИСПДн, а также соответствия реальных условий эксплуатации требованиям по размещению, монтажу и эксплуатации ИСПДн;

– проверка функций или комплекса функций защиты информации от НСД с помощью инструментальных средств контроля, а также путем пробного запуска СЗИ от НСД и наблюдения за их выполнением;

– проверка соответствия примененных параметров настройки элементов системы защиты информации требованиям безопасности информации;

– проверка подсистем защиты информации от НСД, целостности применяемых СЗИ от НСД;

– проверка программной совместимости и корректности функционирования всего комплекса используемых средств вычислительной техники с продукцией, используемой в целях защиты информации;

– испытания системы защиты информации от НСД путем попыток осуществить НСД к тестовой защищаемой информации в обход используемой системы защиты информации.

В ходе проведения испытаний использовались следующие руководящие и нормативно-технические документы:

1) Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

2) Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

3) Руководящий документ Гостехкомиссии России. Защита от несанкционированного доступа к информации. Термины и определения;

4) Руководящий документ Гостехкомиссии России. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации;

5) Руководящий документ Гостехкомиссии России. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации;

6) Руководящий документ Гостехкомиссии России. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности информации;

7) Руководящий документ Гостехкомиссии России. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники;

8) ГОСТ РО 0043-004-2013. Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний.

9) Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена приказом ФСТЭК России №734 от 15 февраля 2008 г.;

10) Методика оценки угроз безопасности информации. Утверждена ФСТЭК России 5 февраля 2021 г.

3. ПОРЯДОК ПРОВЕДЕНИЯ ИСПЫТАНИЙ

3.1. В ходе испытаний проводились следующие мероприятия:

- 1) проверка структуры, состава и условий эксплуатации ИСПДн;
- 2) проверка состояния организации работ и выполнения требований по защите информации;
- 3) проверка ИСПДн на соответствие требованиям безопасности информации;
- 4) проведение испытаний ИСПДн на соответствие требованиям по защите информации от НСД;
- 5) подготовка отчетной документации и оценка результатов испытаний ИСПДн.

РЕЗУЛЬТАТЫ ИСПЫТАНИЙ

В результате проверки организации работ и готовности к функционированию ОИ на соответствие требованиям безопасности информации установлено:

1. Проверка структуры, состава и условий эксплуатации ИСПДн

1.1. Анализ полноты исходных данных и проверка их соответствия реальным условиям размещения, монтажа и эксплуатации ИСПДн

Для проведения испытаний комиссии предъявлены следующие исходные данные и документация:

Таблица 1 – Исходные данные на объект информатизации

№ п/п	Требовалось по Программе и методикам оценки соответствия	Предоставлено Заявителем	Рег. номер
1.	Перечень защищаемых информационных ресурсов с документальным подтверждением уровня конфиденциальности каждого ресурса	Перечень персональных данных, обрабатываемых в информационной системе персональных данных «Граждане»	01-03/25§3 от 22.05.2023
2.	Акт установки уровня защищенности персональных данных при их обработке в ИСПДн	Акт установки уровня защищенности персональных данных при их обработке в информационной системе персональных данных «Граждане»	б/н от 22.05.2023
3.	Оформленный формуляр на ИСПДн	Формуляр на информационную систему персональных данных «Граждане»	01-03/25§2 от 22.05.2023
4.	Состав технических и программных средств, входящих в ИСПДн		
5.	План размещения ОТСС в помещении объекта информатизации		
6.	План контролируемой зоны		
7.	Состав и схемы размещения средств защиты информации		
8.	Перечень программного обеспечения, установленного в ИСПДн		
9.	Сертификаты соответствия требованиям безопасности информации на программные и технические средства ИСПДн, используемые средства защиты	Сертификат соответствия на «Dallas Lock 8.0-K» (копия)	2720 от 25.09.2012
		Сертификат соответствия на «Kaspersky Endpoint Security для Windows» (копия)	4068 от 22.01.2019
		Сертификаты соответствия на «Программный комплекс ViPNet Client 4» (копии)	СФ/124-4062 от 18.05.2021 СФ/525-4189 от 30.12.2021
10.	Описание технологического процесса обработки информации в ИСПДн	Описание технологического процесса обработки информации в информационной системе персональных данных «Граждане»	01-03/25§2 от 22.05.2023
11.	Инструкции администратору безопасности и пользователям ИСПДн	Инструкция администратора безопасности информационных систем персональных данных	01-03/25§3 от 22.05.2023
		Инструкция пользователя информационных систем персональных данных	01-03/25§3 от 22.05.2023
12.	Организационно-распорядительная документация разрешительной системы доступа пользователей ИСПДн к защищаемым информационным ресурсам ИСПДн	Приказ «Об организации работ по обеспечению безопасности персональных данных»	01-03/25§1 от 22.05.2023
		Приказ «Об утверждении списка лиц, имеющих право доступа к ИСПДн «Граждане», и списка помещений ИСПДн «Граждане»	01-03/25 от 22.05.2023
		План внутренних проверок состояния защиты информационной системы персональных данных	01-03/25§3 от 22.05.2023
		Инструкция по физической охране и контролю доступа в помещения	01-03/25§3 от 22.05.2023
		Инструкция обслуживающего персонала информационных систем персональных данных	01-03/25§3 от 22.05.2023
		Инструкция по разграничению доступа пользователей к средствам защиты и информационным ресурсам	01-03/25§3 от 22.05.2023
		Инструкция по учету машинных носителей и регистрации их выдачи	01-03/25§3 от 22.05.2023
		Инструкция по организации антивирусной защиты	01-03/25§3 от 22.05.2023

№ п/п	Требовалось по Программе и методикам оценки соответствия	Предоставлено Заявителем	Рег. номер
		Инструкция по организации парольной защиты	01-03/25§3 от 22.05.2023
		Регламент резервного копирования данных	01-03/25§3 от 22.05.2023
		Матрица доступа пользователей к защищаемым информационным ресурсам информационной системы персональных данных «Граждане»	01-03/25§2 от 22.05.2023
		Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Граждане»	б/н от 22.05.2023
		Акт приемки в эксплуатацию средств защиты информации	4379-01дсп от 05.07.2023
		Адаптированный базовый набор мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных «Граждане»	01-03/25§2 от 22.05.2023
		Положение об обеспечении безопасности персональных данных при их обработке в информационной системе персональных данных «Граждане»	01-03/25§2 от 22.05.2023
		Программа и методики оценки соответствия информационной системы персональных данных «Граждане» требованиям безопасности информации	4379-02дсп от 05.07.2023
13.	Данные о наличии нормативной и методической документации по защите информации и контролю эффективности защиты	Федеральный закон «Об информации, информационных технологиях и о защите информации»	149-ФЗ от 27.07.2006
		Федеральный закон «О персональных данных»	152-ФЗ от 27.07.2006
		Постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»	687 от 15.09.2008
		Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»	1119 от 01.11.2012
		Приказ ФСТЭК России «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»	21 от 18.02.2013
		Приказ ФСБ России «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»	378 от 10.07.2014

Заявителем предоставлены исчерпывающие исходные данные, соответствующие реальным условиям размещения, монтажа и эксплуатации ИСПДн.

1.2. Исследование технологического процесса обработки, хранения и передачи информации
 На ОИ установлен технологический процесс обработки информации («Описание технологического процесса...»). Описание технологического процесса обработки и хранения персональных данных соответствует реальной практике, принятой на рассматриваемом ОИ.

1.3. Определение состава использованных для обработки, хранения и передачи информации ОТСС

В соответствии с Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных на ОИ разработан формуляр. Состав основные технические средства и системы (далее – ОТСС), установленных на объекте, соответствует указанному в формуляре.

2. Проверка состояния организации работ и выполнения требований по защите информации

2.1. Оценка правильности установки уровня защищенности персональных данных при их обработке в ИСПДн

Согласно предоставленным Заявителем документам была проведена проверка соответствия ИСПДн заявленному уровню защищенности персональных данных. Было установлено следующее:

- тип угроз – для информационной системы актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе – 3;
- категории персональных данных, обрабатываемых в информационной системе – специальные категории персональных данных;
- объем обрабатываемых персональных данных – менее чем 100 000;
- принадлежность персональных данных – не являющиеся сотрудниками оператора.

В соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных» ОИ присвоен уровень защищенности персональных данных при их обработке в информационной системе – *третий*.

2.2. Оценка полноты разработки организационно-распорядительной, проектной и эксплуатационной документации. Проверка соответствия их содержания установленным требованиям

В предоставленных документах (см. Таблицу 1) содержатся все необходимые исходные данные об ОИ. Дополнительных документов не требуется.

2.3. Оценка уровня подготовки специалистов, обеспечивающих защиту информации в ИСПДн, и проверку наличия распределения ответственности пользователей ИСПДн за выполнение требований безопасности информации

Специалистом, обеспечивающим защиту информации в ИСПДн, является администратор безопасности, имеющий достаточный уровень подготовки. Ответственность пользователей ИСПДн за выполнение требований безопасности информации регламентируется соответствующими инструкциями.

3. Проверка ИСПДн на соответствие требованиям безопасности информации

3.1. Проверка наличия необходимых документов и соответствия их содержания установленным требованиям, наличия сертификатов соответствия требованиям безопасности информации, проверка их выполнения

СЗИ, используемые в ИСПДн сертифицированы по требованиям безопасности информации. Условия функционирования СЗИ, предусмотренные эксплуатационной и технической документацией к этим средствам, соблюдены.

Таблица 2 – Сертификаты соответствия на СЗИ

№ п/п	Наименование СЗИ	Номер и дата сертификата	Срок действия сертификата
1	Dallas Lock 8.0-K	2720 от 25.09.2012	25.09.2026
2	Kaspersky Endpoint Security для Windows	4068 от 22.01.2019	22.01.2024
3	Программный комплекс VIPNet Client 4	СФ/525-4189 от 30.12.2021	15.09.2024
		СФ/124-4062 от 18.05.2021	18.05.2024

3.2. Проверка выполнения требований безопасности информации к помещению, в котором проводится обработка информации

ОИ размещен в охраняемом здании. Контролируемая зона ограничена ограждающими конструкциями кабинета, в котором расположены ОТСС ОИ.

Визуальный просмотр информации, обрабатываемой на объекте информации посторонними лицами невозможен. На окне помещения, в котором расположен ОИ, имеются жалюзи.

Помещение, в котором установлены ОТСС и расположены машинные носители информации, охраняется, оборудовано дверьми с механическими замками, пожарной сигнализацией.

Помещение признано годным для работы с документами и машинными носителями информации в рабочее время и хранения документов в нерабочее время.

Допуск посторонних лиц в помещения ограничен и без контроля невозможен, согласно инструкции по физической охране и контролю доступа в помещения.

Размещение и монтаж технических средств выполнены в соответствии с требованиями по защите информации.

4. Проведение испытаний ИСПДн на соответствие требованиям по защите информации от НСД

4.1. Проведен контроль защищенности персональных данных, обрабатываемых на ОИ, от НСД («Протокол оценки соответствия...» № 4379-03дсп от 05.07.2023).

Требования по защите информации от НСД выполняются.

ЗАКЛЮЧЕНИЕ

Учитывая вышеизложенное, комиссия считает, что реализованные средства и меры защиты на объекте информатизации – информационной системе персональных данных на базе ПЭВМ «Граждане», установленного в МБДОУ «ДС № 332 г. Челябинска», расположенного по адресу: Челябинская область, город Челябинск, улица Барбюса, дом 144Г, методический кабинет - достаточны и соответствуют требованиям действующих нормативных документов по безопасности информации, предъявляемых к объекту информатизации - информационной системе, обрабатывающей персональные данные *третьего* уровня защищенности.


Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проведена сроком на 3 года и начинает действовать с даты выдачи данного заключения.

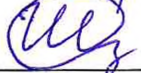
Председатель комиссии



Е.Л. Рублев

Члены комиссии:





К.А. Мисбахова

А.И. Щетин